Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions Are Timely Resolved

February 2001

Reference Number: 2001-20-045

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

February 12, 2001

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions Are Timely Resolved

This report presents the results of our review of unimplemented corrective actions in the Information Systems (IS) organization. In summary, we found that, although actions that were closed during Fiscal Year 1999 effectively addressed Treasury Inspector General for Tax Administration (TIGTA) recommendations, additional emphasis is needed to address critical open actions that have been rescheduled numerous times.

We recommended that the Chief Information Officer (CIO) prioritize critical corrective actions and use monitoring mechanisms to ensure that these actions are timely taken. In addition, we recommended that the CIO designate knowledgeable staff to review responses to TIGTA reports as they are prepared to ensure that corrective actions are clear and concise and provide for measurable completion points.

The CIO agreed with the report recommendations and has taken corrective actions to address them as part of the ongoing IS process improvement efforts. Management's comments have been incorporated into the report where appropriate, and the full text of the response is included as an appendix.

Copies of this report are also being sent to the Internal Revenue Service managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions, or your staff may call Scott Wilson, Associate Inspector General for Audit (Information Systems Programs) at (202) 622-5896.

Table of Contents

Executive Summary .... Page i
Objectives and Scope .... Page 1
Background .... Page 2
Results .... Page 3
  Additional Focus is Needed on Certain Critical Corrective Actions .... Page 4
  Corrective Actions Need to Provide for a Clear Completion Point .... Page 12
Conclusion .... Page 14
Appendix I – Detailed Objectives, Scope, and Methodology .... Page 16
Appendix II – Major Contributors to This Report .... Page 18
Appendix III – Report Distribution List .... Page 19
Appendix IV – Management’s Response to the Draft Report .... Page 20

Executive Summary

In mid-1998, legislation[1] was passed to establish the Treasury Inspector General for Tax Administration (TIGTA) and to define its role in conducting audits and investigations of the Internal Revenue Service (IRS). Prior to that date, the Inspection Service[2] within the IRS conducted audits and investigations of the IRS. The IRS agreed to respond to TIGTA audit reports within 30 days of the issuance of the draft document and to include in its response planned corrective actions and associated implementation dates to address the recommendations made. The Inspector General Act of 1978[3] requires that the TIGTA report semi-annually on critical actions that have not yet been implemented.

During our review, management informed us that the Commissioner had designated financial and management controls as one of five top-level change processes to be pursued in Fiscal Year (FY) 2000. Part of this effort involved prioritization of open corrective actions from responses to TIGTA audit reports. Because this effort was not completed prior to the end of our audit fieldwork, we did not evaluate the results of this prioritization effort. However, we believe that the information in this report can be used in that effort to indicate where increased management oversight is needed.

Our overall objectives were to evaluate the relevance and status of unimplemented corrective actions in the Information Systems (IS) organization that had been rescheduled and to determine whether corrective actions closed during FY 1999 addressed the associated recommendations.

Results

Actions that were closed by IS managers during FY 1999 addressed the associated recommendations and corrective actions were properly completed prior to removal from the tracking system.

However, the IS organization needs to establish better monitoring and prioritization mechanisms so that increased focus is given to ensure critical corrective actions are addressed timely. In addition, oversight should be increased to ensure that the initial responses to TIGTA reports effectively address the recommendations and provide for clear completion points for the actions that IS agrees to take.

---

[1] IRS Restructuring and Reform Act of 1998 (RRA 98), Pub. L. No. 105-206, 112 Stat. 685.

[2] Most of the employees of the Inspection Service became part of the new TIGTA organization as it was established by the RRA 98.

[3] Pub. L. No. 95-452, 92 Stat. 1101, as amended, at 5 U.S.C. app. 3 (1994 & Supp. II 1996).

Additional Focus is Needed on Certain Critical Corrective Actions

The due dates for the 25 open, rescheduled actions we evaluated had been rescheduled a total of 81 times. In addition to these 25 open actions, approximately 39 percent of the corrective actions closed by the IS organization during FY 1999 had been rescheduled. Delays in closing actions ranged from 1 to 7 months.

In evaluating the 25 open, rescheduled actions, we identified 3 areas of significant risk in which the TIGTA has issued multiple reports with similar findings. The IS organization agreed to take actions to address these areas, but the actions remain incomplete as of the end of our fieldwork. Additional oversight is needed in the following critical areas to ensure the associated risk is addressed:

- Management of the IRS' Modernization and Systems Development Programs.
- Security over systems that process taxpayer information.
- Defining and monitoring contracts.

Corrective Actions Need to Provide for a Clear Completion Point

Several of the open, rescheduled corrective actions we reviewed were vaguely written when the response to the original report was prepared. As a result, it was difficult for management to determine when sufficient action had been taken to address the recommendation.

For example, we identified two open corrective actions where sufficient action had been taken to address the recommendations. However, the proposed corrective actions in the responses were vague, and IS management was unable to determine if the actions were completed. We believe these open corrective actions should be closed because the appropriate action to address these recommendations has been taken.

Summary of Recommendations

We recommend that the Chief Information Officer (CIO) prioritize critical corrective actions and use monitoring mechanisms to ensure that these actions are timely taken. In addition, we recommend that the CIO designate knowledgeable staff to review responses to TIGTA reports as they are prepared to ensure that corrective actions are clear and concise and provide for measurable completion points.

Management's Response: The CIO responded that Program Oversight has been realigned into the Strategic Planning and Client Services organization. This has resulted in improved access to executives and promoted greater executive involvement and ownership of audit activities. In addition, the use of program management techniques has been increased to provide executives with information identifying the owner, status, and risks associated with audit activities and open corrective actions. These actions were taken as part of the ongoing IS process to improve program oversight effectiveness.

Objectives and Scope

The overall objectives of this audit were to evaluate the relevance and status of rescheduled corrective actions in IS and to determine whether corrective actions closed during FY 1999 addressed the associated recommendations.

This review was initiated because the Inspector General (IG) Act of 1978[1] requires that the Treasury Inspector General for Tax Administration (TIGTA) report semi-annually on critical actions that have not yet been implemented. The overall objectives of this review were to evaluate the relevance and status of unimplemented corrective actions in the Information Systems (IS) organization that had been rescheduled and to determine whether corrective actions closed during Fiscal Year (FY) 1999 addressed the associated recommendations.

To complete this review, we selected and evaluated 25 IS actions that had been rescheduled from their original due dates and were open at the time of our review. We reviewed them to determine their criticality and to evaluate reasons for the delays in implementation. In addition, we selected and reviewed a sample of 36 actions (from a total of 68) that had been closed during FY 1999 to determine whether actions were appropriately taken as indicated when the actions were closed.

We conducted this review between February and July 2000. This audit was performed in accordance with *Government Auditing Standards*. We interviewed key personnel and reviewed documentation at the following sites:

- The Office of the Chief Information Officer in New Carrollton, Maryland.
- The Office of the Chief Financial Officer in Washington, DC.

Details of our audit objectives, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

---

[1] Pub. L. No. 95-452, 92 Stat. 1101, as amended, at 5 U.S.C. app. 3 (1994 & Supp. II 1996).

Background

The TIGTA and the former Inspection Service[2] have conducted numerous audits of the Internal Revenue Service's (IRS) IS organization over the past several years and issued reports with recommendations for corrective actions on issues identified during the reviews. The IRS agreed to respond to TIGTA audit reports within 30 days of the issuance of the draft document and to include in its response planned corrective actions and associated implementation dates to address the recommendations made.

The Treasury Department uses the Inventory, Tracking and Closure (ITC) system to track TIGTA recommendations and the IRS' related corrective actions. The ITC system tracks when a corrective action should be implemented and the official responsible for implementation. Each month, the TIGTA receives a list of those actions that are past due or have rescheduled implementation dates. This audit focused on actions in these categories that relate to the IRS' IS activities.

In FY 2000, the IRS established an effort to prioritize its current inventory of corrective actions from TIGTA audits. This was one of the major objectives set by the Commissioner when he established the new Financial Management Controls Executive Steering Committee, and when he designated financial and management controls as one of five top-level change processes to be pursued in FY 2000. In addition to the prioritization, the IRS was attempting to filter out corrective actions that may have been duplicated by other efforts, addressed through the organizational or technology modernization, or no longer made sense in its analysis of costs and benefits.

---

[2] The TIGTA was created and the former Inspection Service was abolished by the IRS Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685. This Act also defines the TIGTA's role in conducting audits and investigations of the IRS.

Because this effort was not completed prior to the end of our audit fieldwork, we did not evaluate the results of this prioritization effort. However, we believe that the information in this report can be used in that effort to indicate where increased management oversight is needed.

The IG Act does not provide for elimination of previously agreed-upon corrective actions from the ITC system, even if they meet the IRS' above-mentioned criteria. The TIGTA has established a process in which the IRS can request the elimination of individual unimplemented corrective actions, if requests are made via a memorandum to the TIGTA's Office of Audit. This process is required only if the action to be eliminated from the ITC system has not been implemented. If the action has been implemented, the IRS can close it from the ITC system without TIGTA approval.

Results

Corrective actions that were closed by IS management in FY 1999 appropriately addressed the related TIGTA/Inspection recommendations. The 36 corrective actions we evaluated were also properly completed prior to removal from the ITC system.

However, our evaluation of open and rescheduled corrective actions indicated that the IS organization needs to establish better monitoring and prioritization mechanisms. Increased focus is needed to ensure critical corrective actions are timely addressed.

In addition, oversight should be increased to ensure that the initial responses to TIGTA reports effectively address the recommendations and provide for clear completion points for the actions that the IS organization agrees to take.

Additional Focus is Needed on Certain Critical Corrective Actions

Our evaluation of open and rescheduled actions indicated that IS executives need to increase their focus on certain critical actions that have been addressed in multiple TIGTA reports. To identify this issue, we selected and evaluated the 25 actions that had been rescheduled from a list of 68 open actions as of December 31, 1999. These 25 actions were included in responses to 11 audit reports issued to the IS organization between April 1997 and September 1999. During the time period of our review, 2 of the 25 actions were closed; however, we included them in our review because they were closed during the final portion of our audit fieldwork.

The 25 open actions we evaluated had been rescheduled a total of 81 times. In addition, approximately 39 percent of the corrective actions closed by the IS organization during FY 1999 had been rescheduled, with delays ranging from 1 to 7 months.

TIGTA audits of the IS organization identified recurring issues of significant risk in three areas.

In our analysis of these 25 actions, we identified 3 areas of significant risk in which the TIGTA has issued various reports with similar findings. The IS organization has agreed to take actions to address these areas, but the actions remain incomplete as of the end of our fieldwork. Actions are needed in each of these areas to address the associated risk. The areas of significant risk that were addressed by various open actions are:

- Management of the IRS' Modernization and Systems Development Programs.
- Security over systems that process taxpayer information.
- Defining and monitoring contracts.

Problems in any one of these areas could result in significant loss or potential embarrassment to the IRS. Successful management of the IRS' systems development programs and attention to detail in defining and monitoring contracts are critical to the success of the modernization effort. In addition, security over taxpayer data is becoming a bigger concern every day to the Congress and the general public.

Executives in the CIO's organization believe that in the majority of cases, the actions were delayed because changes occurred in the area audited after the original report was issued and, therefore, the delays were for legitimate reasons.[3] However, our discussions with various managers indicated that some of these actions were delayed because management did not always place the appropriate emphasis on timely correcting them.

Management of the IRS' Modernization and Systems Development Programs

Two of the open, rescheduled corrective actions we evaluated were related to a 1999 audit[4] that reported weaknesses in the management of the IRS' systems development programs. The first action included the use of Investment Decision Management Principles and Business Cases, while the second was focused on the implementation of general program management principles to address cost, schedule, technical performance, and risk management. The IRS originally agreed to take (and close) these actions by November 1999 but, as of the end of our fieldwork, the actions had still not been closed.

The IRS lacked comprehensive decision criteria for controlling and evaluating systems modernization projects.

Developing processes to address these agreed-to actions is critical to the success of the IRS' Modernization Program. The Clinger-Cohen Act[5] and current IRS policies and procedures require the use of a disciplined, decision-making process for planning, managing, and controlling the acquisition of information systems and services. In order to assess the merits of new systems before implementing them, the IRS generally produces a business case. A business case is a management tool that documents the essential aspects of an information technology project. Best practices in the management of information technology investments require that a business case be continuously updated to represent the current situation.

---

[3] We did not evaluate each of the individual delays for reasonableness because of the number of delays that occurred and the technical nature of some of the delays.

[4] *Effectiveness of the IRS Management of the Customer Service Call Router Pilot,* (Reference Number 094602, dated September 1999).

[5] Pub. L. 104-106, February 10, 1996.

TIGTA audit work in the modernization area indicates that the IRS has made progress in the development of processes to follow in making investment management decisions. However, a TIGTA audit[6] indicated that these processes were only recently being incorporated into the IRS' methodology to manage its business change. Until these processes are fully incorporated and documented, it will be difficult to ensure that they are consistently used in the modernization effort.

Another recent TIGTA audit[7] reported weaknesses in program management of the systems modernization effort, in areas such as program management staffing needs, performance monitoring, and risk management. Several of these issues were similar to the second open action from the 1999 report. Although the IS organization has taken significant steps to address some of these weaknesses, this recent audit report indicated that it has struggled in establishing the program management office. In addition, delays have been experienced in the implementation of the Enterprise Life Cycle, the IRS' new business change methodology.

With the high visibility and significant funding to be allocated to the modernization efforts, additional attention and focus is needed to ensure the agreed upon actions are taken quickly.

---

[6] *Implementation of the New Methodology for Systems Modernization Needs Increased Focus and Support,* (Reference Number 2001-20-015 dated November 2000).

[7] *Significant Risks Need To Be Addressed to Ensure Adequate Oversight of the Systems Modernization Effort,* (Reference Number 2000-20-099, dated June 2000).

Security over systems that process taxpayer information

Six of the open, rescheduled actions we reviewed were centered around security weaknesses in systems that process taxpayer information. Although the weaknesses were reported in two separate reports covering the Service Center Mainframe Consolidation (SCMC)[8] and the Electronic Fraud Detection System (EFDS),[9] both included information that these systems had not been adequately certified and accredited. Certain parts of the SCMC and the EFDS are currently operating using an Interim Authority to Operate,[10] rather than having a completed certification and accreditation performed.

A recent TIGTA audit reported that approximately 90 percent of sensitive systems remain uncertified and unaccredited.

More recent TIGTA work[11] reported continuing problems in the areas of certification and accreditation. Approximately 90 percent (232 of 258) of the systems listed on the inventory of sensitive systems in January 2000 were not currently certified and accredited. Responsible executives had granted temporary authorities to operate 143 of the uncertified systems, but had accepted no accountability for the security risks of operating the other 89 systems. In addition, security certification continues to be reported as a material weakness by the IRS.

---

[8] *Readiness for Service Center Mainframe Consolidation*, (Reference Number 085812, dated September 1998).

[9] *Review of the Electronic Fraud Detection System (EFDS),* (Reference Number 093009, dated June 1999).

[10] Three typical cases where an interim approval to operate may be employed are:

- A new system is in an advanced test phase and must use some operational data for final design and testing.
- An initial survey has concluded that there are no apparent security problems that would allow unauthorized persons to access data in a system, but there has not been sufficient time for rigorous hardware/software testing.
- The configuration of an operational system has been altered, and an initial security evaluation does not reveal any severe problems.

[11] *Certifying the Security of Internal Revenue Service Computer Systems Is Still a Material Weakness*, (Reference Number 2000-20-092, dated June 2000).

The EFDS has audit trail weaknesses which have not all been addressed.

A second open security issue we evaluated centered around the EFDS audit trail. An audit trail is a required control to detect potential unauthorized disclosure of sensitive information. Our review of open, rescheduled actions identified three actions that remain unimplemented. These relate to the need to enhance the audit trail for the EFDS.

Although the IS organization took some actions to improve the audit trail, it agreed to take further actions to record accesses to taxpayer data through secondary sources and to include date-range fields and service center site fields in the audit trail reports. These actions were to have been completed in April 2000. However, as of the end of our fieldwork, they still had not been finalized, and these audit trail weaknesses remain.

In addition, the EFDS project office agreed to coordinate the audit trail efforts with TIGTA's Strategic Enforcement Division to develop specific audit trail requirements necessary for use in a system designed to identify unauthorized system accesses. However, the effort, which was originally scheduled to be completed in April 2000, has been delayed until early 2001.

Certifying that adequate security controls have been developed and accrediting that the risks of security breaches have been adequately reduced are two primary controls for ensuring security over taxpayer data. A lack of certification and accreditation can result in security weaknesses going undetected and taxpayer data being at risk of unauthorized disclosure. An audit trail is a key control to detect potential breaches of system security. Addressing these security weaknesses is critical to protecting sensitive taxpayer information.

Defining and monitoring contracts

In our analysis of rescheduled corrective actions, we identified six open actions that related to defining contract requirements and validating contractor performance. These actions were reported in three separate reports[12] and covered two different contracts. Recent TIGTA work on modernization contracts[13] indicated that some of these problems continue to occur in the modernization area.

The IRS could potentially save significant amounts of money by defining and validating delivery orders.

Issues related to defining and validating delivery order requirements for the SCMC contract were originally reported in 1998. The IS organization agreed to revise its project management plan and to assign additional resources to validate these requirements by January 1, 1999. As of the end of our audit fieldwork, these actions still had not been completed even though follow-up work in this area in 1999[14] indicated that $19 million was saved by partially validating these orders.

That follow-up audit also indicated that the Project Office should have established full-time Government Task Managers and support staff to monitor and verify contractor activities because over $7 million was identified as work performed by the contractor without authorization from the Contracting Officer. Although these efforts were originally scheduled for completion in March 2000, this action was still open at the end of our audit fieldwork.

---

[12] *Readiness for Service Center Mainframe Consolidation (SCMC)*, (Reference Number 085812, dated September 1998).
Service Center Mainframe Consolidation (SCMC) Project Has Made Significant Progress, But Project Execution and Administration Risks Remain, (Reference Number 199920068, dated September 1999).
Review of the Integration Support Contract (ISC), (Reference Number 084803, dated July 1998).

[13] *Administration of the PRIME Contract Can Be Improved*, (Reference Number 2000-10-138, dated September 2000).

[14] *Service Center Mainframe Consolidation (SCMC) Project Has Made Significant Progress, But Project Execution and Administration Risks Remain*, (Reference Number 199920068, dated September 1999).

A TIGTA report issued in September 2000 identified that 25 of 29 modernization task orders had been issued without being definitized.

A recent TIGTA report[15] identified similar issues with defining contracts in the systems modernization program. At the time that fieldwork for that report was conducted, 25 of the 29 modernization task orders had been issued undefinitized.[16] An undefinitized task order allows the contractor to be reimbursed for allowable costs[17] up to a limitation amount stated in the task order. However, the government's negotiating position is diminished as work is completed under an undefinitized task order since the contractor must be paid allowable costs incurred. Therefore, the contractor has little incentive to quickly negotiate terms and conditions.

In a separate audit,[18] two actions addressing monitoring of contractor performance remain open and have been rescheduled at least four times. One recommendation was made to ensure that an in-depth analysis of contractor labor hours and costs be performed prior to payment of the invoices. The other involved the monitoring of government-furnished equipment and information provided to the contractor. The IS organization originally planned to complete these actions by January 1, 1999, but rescheduled the due date to October 1, 2000. Because our fieldwork ended in July 2000, we did not verify whether the action was taken by the rescheduled date.

Defining contracts and monitoring contractor performance is a critical area because of the large dollar value of some of these contracts, as well as the potential for loss of value if these contracts are not effectively defined and monitored. In addition, it is a sensitive area which attracts significant attention from the media and taxpayers if abuse is identified. Further delays in implementing key controls as recommended in these reviews could result in money being spent for items that the IRS may never receive or work that may never be performed.

---

[15] *Administration of the PRIME Contract Can Be Improved*, (Reference Number 2000-10-138, dated September 2000).

[16] Undefinitized – A contractual action in which the terms and conditions have not been agreed upon by all parties.

[17] Allowable costs are those costs the contractor is permitted to be reimbursed by the government for performance of a contract.

[18] *Review of the Integration Support Contract (ISC),* (Reference Number 084803, dated July 1998).

Recommendations

To ensure that sufficient focus is provided to significant corrective actions, we recommend that the Chief Information Officer (CIO):

1. Prioritize critical corrective actions when responses to audit reports are prepared.
2. Develop and use project management techniques to more effectively monitor the implementation status of corrective actions so that increased attention can be given when critical actions are delayed.

Management's Response: The IS organization took the following actions as part of its ongoing process to improve program oversight effectiveness:

- Improved organizational placement by realigning Program Oversight into the Strategic Planning and Client Services organization. This realignment resulted in improved access to top level executives and promoted executive involvement throughout the oversight process, including greater emphasis on executive ownership of audit activities and participation in developing, prioritizing, and assessing the effectiveness of corrective actions.
- Increased use of program management techniques to provide executives with information, which easily identifies the owner, status, and risks associated with audit activities and open corrective actions. The IS organization is involving appropriate executives in assessing the effectiveness of implemented corrective actions by conducting meetings to review the status/risk tools with the Director, Strategic Planning and Client Services, the Deputy Chief Information Officers and the CIO. The IS organization is also using Red-Yellow-Green

Dashboard reports and 30-Day View reports for both audit activities and corrective actions to highlight areas that require executive involvement to mitigate the risks.

Corrective Actions Need To Provide for a Clear Completion Point

The completion point for several corrective actions was vague when the response to the original report was prepared.

Several corrective actions were written in a vague manner when the response to the original report was prepared. As a result, it was difficult for management to determine when sufficient action had been taken to address the recommendation.

For example, on the original SCMC report,[19] the IS organization responded to a recommendation related to contingency planning for critical human resources by listing several actions it planned to take to address this issue. These actions included considering using vendor support, detailing employees into the area on a limited basis, remote operations, and other government agency/vendor support. Because this action was so broad, IS management officials were unable to determine when sufficient action had been taken to close the corrective action. A subsequent TIGTA audit[20] found that sufficient actions had been taken to address this issue and, as a result, we believe this action can be closed.

Another action from the first SCMC report involved conducting vendor site surveys prior to undertaking consolidation efforts. Since the time this was originally reported, the IS organization established a site survey process, and these surveys were being conducted in a consistent and timely manner. However, the IS organization has kept this action open because all of the surveys have not yet been completed. We believe that management should request this action be considered for closure based on the fact that a process has been established and is being consistently followed.

---

[19] *Readiness for Service Center Mainframe Consolidation, (SCMC),* (Reference Number 085812, dated September 1998).

[20] *Significant Progress Has Been Made in Consolidating Mainframe Computer Operations, But Risks Remain,* (Reference Number 2000-20-085, dated June 2000).

The IRS issued internal guidance dated October 15, 1999, on preparation of corrective action plans in response to TIGTA audit reports. This guidance indicates that, "Each corrective action should be concise, but contain sufficient detail to ensure that the finding and recommendation are addressed. The projected implementation date or completion date will be included for each action."

Discussions with management indicated that because time frames are tight in preparing and issuing responses to draft reports, the CIO's office usually does not receive the response until a day or two before it is due to the TIGTA. As a result, he and/or his staff do not usually have the opportunity to conduct a thorough review of the proposed corrective actions before the response is issued. In addition, the liaisons who assist in preparing responses to reports do not always have a clear understanding of some of the more technical issues involved in certain IS corrective actions.

If corrective actions are not written concisely and clearly, IRS management may have a difficult time recognizing when sufficient work has been completed to address the finding and recommendation. As a result, actions that could legitimately be closed may remain open on the ITC system beyond the point when the action was completed.

Recommendation

To ensure corrective actions provide for a clear completion point, we recommend that the CIO:

3. Designate knowledgeable staff members to review corrective actions prior to the issuance of the report

response to ensure the actions are clear and concise and provide for measurable completion points.

Management's Response: The IS organization took the following actions as part of its ongoing process to improve program oversight effectiveness:

- Improved organizational placement by realigning Program Oversight into the Strategic Planning and Client Services organization. This resulted in improved access to top level executives and promoted executive involvement throughout the oversight process, including greater emphasis on executive ownership of audit activities and participation in developing, prioritizing, and assessing the effectiveness of corrective actions.
- Increased use of program management techniques to provide executives with information, which easily identifies the owner, status, and risks associated with audit activities and open corrective actions. The IS organization is involving appropriate executives in assessing the effectiveness of implemented corrective actions by conducting meetings to review the status/risk tools with the Director, Strategic Planning and Client Services, the Deputy Chief Information Officers and the CIO. The IS organization is also using Red-Yellow-Green Dashboard reports and 30-Day View reports for both audit activities and corrective actions to highlight areas that require executive involvement to mitigate the risks.

Conclusion

The IS organization is appropriately taking corrective actions prior to closing them off the tracking system. However, certain actions in critical areas like program management, security, and contract monitoring remain open and continue to be rescheduled. Findings in these critical areas are continuing to be reported by the

TIGTA. The CIO needs to ensure that additional focus is given to taking these actions.

In addition, the CIO needs to establish better monitoring and prioritization systems and ensure that initial responses provide for clear, concise actions and completion points. Additional emphasis in these areas will help ensure that critical actions are taken appropriately and timely, and that actions are closed when completed.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives of this review were to evaluate the relevance and status of unimplemented corrective actions in the Information Systems (IS) organization that had been rescheduled, and to determine whether the corrective actions closed during Fiscal Year (FY) 1999 addressed the associated recommendations.

I. To evaluate the controls and the processes that the Internal Revenue Service (IRS) uses to implement Treasury Inspector General for Tax Administration (TIGTA) recommendations, we:

   A. Interviewed IRS management to ascertain how implementation of corrective actions was tracked and controlled.

   B. Evaluated the controls and the processes used to update the Inventory, Tracking and Closure (ITC) system information.

II. To identify past due and rescheduled corrective actions and to determine if the actions were still appropriate, we:

   A. Obtained ITC system information from the TIGTA's Office of Management and Policy (OMP) showing all past due and rescheduled corrective actions as of December 31, 1999.

      1. Identified the 33 past due and rescheduled actions with responsible officials in the IS organization. We later eliminated the five actions that were originally considered past due because a response to the associated report was received and it did not indicate that these actions needed to be delayed. In addition, we eliminated three other actions that were closed soon after our fieldwork began. This resulted in 25 actions that we used for our further analysis.

      2. Obtained and evaluated the ITC system reports from the OMP and compared them to the ITC database and the related audit reports and determined whether the information was accurate and reconcilable.

      3. Reviewed the related audit reports with the recommendations to gain a familiarity with the audit issues.

      4. Interviewed the TIGTA audit managers who issued the audit reports to determine the basis for the recommendations issued and to get their opinions on the current validity of the recommendations.

   5. Interviewed the IRS officials responsible for the recommendations to get their opinions on the current validity of the open recommendations.

B. Evaluated the past due and rescheduled unimplemented corrective actions and the results of the interviews with IRS and TIGTA management and determined whether the corrective actions were still appropriate.

III. To evaluate the progress and the current status of actions on IS corrective actions that were still appropriate, we:

A. Interviewed the responsible officials in the IS organization to determine what progress had been made on implementing the corrective actions.

B. Identified the appropriate method to measure the potential impact of delaying closure of these issues.

IV. To evaluate corrective actions taken during FY 1999 and to determine whether the corrective actions addressed the recommendations, we:

A. Obtained a listing of all the corrective actions that were closed during FY 1999.

   1. Identified all of the closed corrective actions that were the responsibility of IS officials.

   2. Obtained a copy of all the ITC system reports for the closed corrective actions and the related TIGTA audit reports.

   3. Eliminated all Year 2000 (Y2K) reports from the sample due to the "one-time" nature of that event and the associated IRS activities.

   4. Selected a judgmental sample of 36 closed actions (53 percent of the 68 actions that were closed) from the reports with actions that were closed during FY 1999.

V. Analyzed and reviewed documentation for the sample of closed corrective actions and discussed the closed corrective actions with IS management to determine if the corrective actions satisfied the recommendations.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Scott Macfarlane, Director
Tammy L. Whitcomb, Audit Manager
Charles R. Winn, Senior Auditor
Albert C. Greer, Jr., Auditor
Suzanne Noland, Auditor

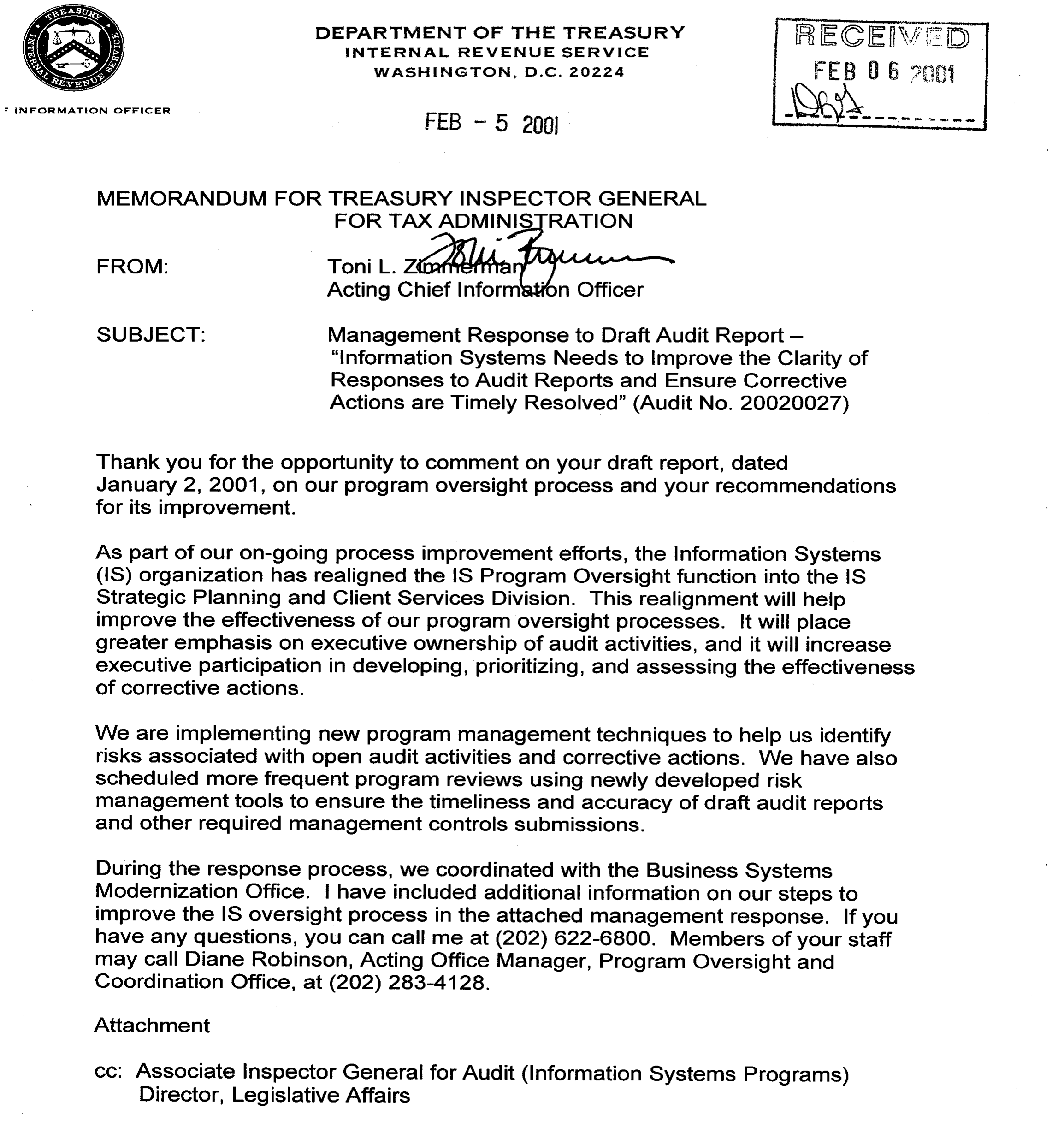
Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief Counsel CC
Chief Financial Officer N:CFO
National Taxpayer Advocate TA
Associate Commissioner Business Systems Modernization B
Assistant Deputy Commissioner Modernization N:ADC:MOD
Director, Information Resources Management IS:IR
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Director, Security Evaluation and Oversight IS:SPO:S
Director, Tax Administration Coordination N:ADC:T
Office of Management Controls N:CFO:F:M
Audit Liaisons:
    Chief Information Officer IS
    Associate Commissioner Business Systems Modernization B

Appendix IV

Management's Response to the Draft Report



INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
FEB 06 2001

FEB - 5 2001

MEMORANDUM FOR TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

FROM: Toni L. Zimmerman
Acting Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – "Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions are Timely Resolved" (Audit No. 20020027)

Thank you for the opportunity to comment on your draft report, dated January 2, 2001, on our program oversight process and your recommendations for its improvement.

As part of our on-going process improvement efforts, the Information Systems (IS) organization has realigned the IS Program Oversight function into the IS Strategic Planning and Client Services Division. This realignment will help improve the effectiveness of our program oversight processes. It will place greater emphasis on executive ownership of audit activities, and it will increase executive participation in developing, prioritizing, and assessing the effectiveness of corrective actions.

We are implementing new program management techniques to help us identify risks associated with open audit activities and corrective actions. We have also scheduled more frequent program reviews using newly developed risk management tools to ensure the timeliness and accuracy of draft audit reports and other required management controls submissions.

During the response process, we coordinated with the Business Systems Modernization Office. I have included additional information on our steps to improve the IS oversight process in the attached management response. If you have any questions, you can call me at (202) 622-6800. Members of your staff may call Diane Robinson, Acting Office Manager, Program Oversight and Coordination Office, at (202) 283-4128.

Attachment

cc: Associate Inspector General for Audit (Information Systems Programs)
Director, Legislative Affairs

Attachment

Management Response to the Draft Audit Report – "Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions are Timely Resolved" (Audit No. 200020027)

Recommendation #1

To ensure that sufficient focus is provided to significant corrective actions, we recommend that the Chief Information Officer (CIO):

1. Prioritize critical corrective actions when responses to audit reports are prepared.

Assessment of Cause

As Information Systems management creates corrective actions, it prioritizes them based on resource availability, current long-term and short-term commitments and customer requirements. We need to strengthen management and executive oversight of the development, closure and assessment of effective corrective actions.

Corrective Action #1

Information Systems took the following actions as part of our on-going process to improve program oversight effectiveness:

1. Improved organizational placement by realigning Program Oversight into the Strategic Planning and Client Services. This resulted in improved access to top level executives and promoted executive involvement throughout the oversight process, including greater emphasis on executive ownership of audit activities and participation in developing, prioritizing, and assessing the effectiveness of corrective actions.

2. Increased use of program management techniques to provide executives with information, which easily identifies the owner, status, and risks associated with audit activities and open corrective actions. We are involving appropriate executives in assessing the effectiveness of implemented corrective actions by conducting meetings to review the status/risk tools with the Director, Strategic Planning and Client Services, the Deputy Chief Information Officers and the Chief Information Officer. We are also using Red-Yellow-Green Dashboard reports and 30-Day View reports for both audit activities and corrective actions to highlight areas that require executive involvement to mitigate the risks.

Attachment

Management Response to the Draft Audit Report – "Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions are Timely Resolved" (Audit No. 200020027)

Implementation Dates Corrective Action #1

Completed: January 9, 2001
Implement improved program management
Techniques and increase executive involvement.

Responsible Official(s) for Corrective Action #1

Chief Information Officer IS
Director, Strategic Planning and Client Services IS:SP

Corrective Action #1 Monitoring Plan

To strengthen the oversight program, management in the Strategic Planning and Client Services will continue planned status/risk meetings to assess the effectiveness of the oversight program and provide feedback for the IS functions and executives. They will make changes to the program, as needed.

Recommendation #2

To ensure that sufficient focus is provided to significant corrective actions, we recommend that the Chief Information Officer (CIO):

2. Develop and use project management techniques to more effectively monitor the implementation status of corrective actions so that increased attention can be given when critical actions are delayed.

Assessment of Cause

As Information Systems management creates corrective actions, it prioritizes them based on resource availability, current long-term and short-term commitments and customer requirements. We need to strengthen management and executive oversight of the development, closure and assessment of effective corrective actions.

Corrective Action #2

Information Systems took the following actions as part of our on-going process to improve program oversight effectiveness:

Attachment

Management Response to the Draft Audit Report – "Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions are Timely Resolved" (Audit No. 200020027)

1. Improved organizational placement by realigning Program Oversight into the Strategic Planning and Client Services. This resulted in improved access to top level executives and promoted executive involvement throughout the oversight process, including greater emphasis on executive ownership of audit activities and participation in developing, prioritizing, and assessing the effectiveness of corrective actions.

2. Increased use of program management techniques to provide executives with information, which easily identifies the owner, status, and risks associated with audit activities and open corrective actions. We are involving appropriate executives in assessing the effectiveness of implemented corrective actions by conducting meetings to review the status/risk tools with the Director Strategic Planning and Client Services, the Deputy Chief Information Officers and the Chief Information Officer. We are also using Red-Yellow-Green Dashboard reports and 30-Day View reports for both audit activities and corrective actions to highlight areas that require executive involvement to mitigate the risks.

Implementation Date Corrective Action #2

Completed: **January 9, 2001**
Implement improved program management
techniques and increase executive involvement

Responsible Official(s) for Corrective Action #2

Chief Information Officer IS
Director, Strategic Planning and Client Services IS:SP

Corrective Action #2 Monitoring Plan

To strengthen the oversight program, management in the Strategic Planning and Client Services will continue planned status/risk meetings to assess the effectiveness of the oversight program and provide feedback for the IS functions and executives. They will make changes to the program, as needed.

Recommendation #3

To ensure corrective actions provide for a clear completion point, we recommend that the CIO:

Attachment

Management Response to the Draft Audit Report – "Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions are Timely Resolved" (Audit No. 200020027)

3. Designate knowledgeable staff members to review corrective actions prior to the issuance of the report response to ensure the actions are clear and concise and provide for measurable completion points.

Assessment of Cause

As Information Systems management creates corrective actions, it prioritizes them based on resources availability, current long-term and short-term commitments. We need to strengthen management and executive oversight of the development, closure and assessment of effective corrective actions.

Corrective Action #3

Information Systems took the following actions as part of our on-going process to improve program oversight effectiveness:

1. Improved organizational placement by realigning Program Oversight into the Strategic Planning and Client Services. This resulted in improved access to top level executives and promoted executive involvement throughout the oversight process, including greater emphasis on executive ownership of audit activities and participation in developing, prioritizing, and assessing the effectiveness of corrective actions.

2. Increased use of program management techniques to provide executives with information, which easily identifies the owner, status, and risks associated with audit activities and open corrective actions. We are involving appropriate executives in assessing the effectiveness of implemented corrective actions by conducting meetings to review the status/risk tools with the Director, Strategic Planning and Client Services, the Deputy Chief Information Officers and the Chief Information Officer. We are also using Red-Yellow-Green Dashboard reports and 30-Day View reports for both audit activities and corrective actions to highlight areas that require executive involvement to mitigate the risks.

Implementation Date Corrective Action #3

Completed: January 9, 2001
Implement improved program management
techniques and increase executive involvement

Attachment

Management Response to the Draft Audit Report – "Information Systems Needs to Improve the Clarity of Responses to Audit Reports and Ensure Corrective Actions are Timely Resolved" (Audit No. 200020027)

Responsible Official(s) for Corrective Action #3

Chief Information Officer IS
Director, Strategic Planning and Client Services IS:SP

Corrective Action #3 Monitoring Plan

To strengthen the oversight program, management in the Strategic Planning and Client Services will continue planned status/risk meetings to assess the effectiveness of the oversight program and provide feedback for the IS functions and executives. They will make changes to the program, as needed.